

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-157751  
(43)Date of publication of application : 03.06.2004

(51)Int.Cl. G06F 12/14  
G06F 9/46

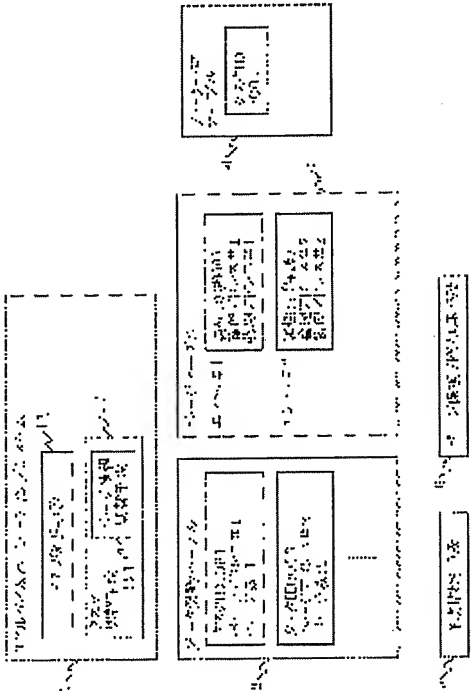
(21)Application number : 2002-322604 (71)Applicant : NEC CORP  
(22)Date of filing : 06.11.2002 (72)Inventor : FUKAGAWA YOSHIMI

(54) SYSTEM, PROGRAM, AND METHOD FOR PROTECTING DATA

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system, a program, and a method for protecting a writable area held by each program in a system using an operating system such as a real time operating system loading all programs and data on a main storage memory and sharing a memory space between all the programs.

SOLUTION: An initial setting means 5 sets page information held by each task in a data protection table 2 by a task unit to form a page table 3 on the basis of this information, sets each page attribute in protection, and checks whether protected page information matching the task in operation in the data protection table 2 includes an excluded page or not when a page protection exclusion means 6 is called. If the excluded page is included, the page attribute is allowed, and a task ID is registered in a data permission table 4. If the excluded page is not included, the task in operation is suspended, and when a task switching means 12 switches the task, the protected page information is acquired from the data protection table 2 by using a registered task ID, and the attribute of the matching page is returned to a protected condition.



LEGAL STATUS

[Date of request for examination] 17.10.2005  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the  
examiner's decision of rejection or application  
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

In case this invention uses such an operating system especially about the system which protects the data of a program in case the operating system which loads all programs and data on the primary storage, and is sharing room between all programs like a real time operating system is used, the program from which the data of a program are protected, and the protection approach, it relates to the data-protection system which prevents that other programs and the data of a task are rewritten by the fault of a program etc., a data-protection program, and the data-protection approach.

[0002]

[Description of the Prior Art]

Conventionally, in the operating system equipped with virtual memory, it has an address space for every process, and a page table is updated for every change of a process. It does not break out that this rewrites the data of a current process to another process.

[0003]

However, since the real time operating system used with real-time system needs high-speed processing, it loads all programs and data on primary-storage memory, and is sharing room between all programs.

[0004]

Moreover, the address of a program and data is in agreement with a physical address.

[0005]

Therefore, access to the unsuitable address by the fault of a program is undetectable.

[0006]

There is a memory protective device as a technique of solving a problem similar to this on the other hand (for example, patent reference 1 reference).

[0007]

Two or more memory protection information storage means by which this memory protective device stores protection information corresponding to each memory block, It has a current key information storage means to memorize the attribute information about a certain memory block. Before accessing a certain memory block, a protection key is beforehand set as the memory protection information storage means corresponding to this memory block. Whenever it sets the attribute key about this memory block as the current key information storage means and there is access to memory block, are concurrent with this memory access. The protection key of memory block corresponding to this memory address within a memory protection storage means is compared with the attribute key within a current key information storage means. If the conditions defined beforehand are satisfied and it will not be satisfied [ permit this memory access and ], it is the memory protective device which notifies outside that forbade this memory access and the violation of access arose.

[0008]

Access will be permitted, if the memory-block upper address of a protection key register is in agreement here and the process ID of a current key register and a protection key register is in agreement.

[0009]

Moreover, a memory protection table is separated from the general memory which stores memory block, and a memory protection check is performed, without reducing a throughput by the ability being made to carry out concurrent access of a memory protection table and the memory block.

[0010]

[Patent reference 1]

JP,5-134930,A (a paragraph [0008], [0014], [0054] - [0056])

[0011]

[Problem(s) to be Solved by the Invention]

Therefore, in the above-mentioned memory protective device, each entry of a memory protection table holds the process ID, and memory size becomes large from the case where a 1-bit guard bit is prepared, and general memory is separated another memory, and there is a problem said that the parting amount of resources increases.

[0012]

The protection system of the data in small equipments, such as a personal digital assistant, at least is not turned to.

[0013]

Moreover, before a setup of the process ID to a memory protection table etc. accesses a certain memory block, it is set up beforehand, but there is no means performed by summarizing a setup of all entries by initial setting, it loads [ no ] programs to a primary storage in early stages, and after it secures a data area, it turns to the system which operates with the memory map.

[0014]

The purpose of this invention is a system using the operating system which loads all programs and data on primary-storage memory, and is sharing room between all programs like a real time operating system, and offers the program and approach the system which protects the field (it is rewritable) which each program owns, and for protecting.

[0015]

A data protection system, a protection program, and an approach applicable also to a small terminal and a small information processor are offered without being able to lessen the increment in the processing time about primary-storage access, and changing an operating system subordinate's program especially.

[0016]

[Means for Solving the Problem]

In the system of operating system use by which the 1st data protection system of this invention shares one room between a program by initial setting of a system A means to set the page information on the primary storage which each task owns as a data protection table per task, The page table with which the entry corresponding to the address is referred to at the time of primary-storage access is created based on the information on said data protection table, and it is characterized by having a means to set the attribute of each page of this as a protection state.

[0017]

An initialization means for the 2nd data protection system of this invention to set up said data protection table, to create said page table in said 1st data protection system based on this information, and to set the attribute of each page as a protection state, It has the page protection exception-handling means which will be called if a write-in demand to the page of a protection state is, and a task change means. Said page protection exception-handling means A means to confirm whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, A means to register it if said page is included as a result of a check, the attribute of the applicable page of a page table will be made into an authorized state and said task ID which was being performed will not be registered into the data authorization table 4, It has the means which makes hibernation the task which was being performed as a result of said check if said page was not included. Said task change means In case a task is changed, the protection page information of the task to which a data protection table corresponds if Task ID is registered into the data authorization table is acquired. The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having a means to eliminate the task ID of said data authorization table.

[0018]

An initialization means for the 3rd data protection system of this invention to set up said data protection table, to create said page table in said 1st data protection system based on this information, and to set the attribute of each page as a protection state, It has the page protection exception-handling means which will be called if a write-in demand to the page of a protection state is, and a task change means. Said page protection exception-handling means A means to confirm whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, A means to make the attribute of the page of a page table concerned into an authorized state if said page is included as a result of a check, and to register the identification information of the page into a data authorization table, It has the means which makes hibernation the task which was being performed if said page was not included as a

result of the check. Said task change means If page identification information is registered into the data authorization table in case a task is changed, the attribute of the page to which a page table corresponds will be returned to a protection state, and it will be characterized by having a means to eliminate said page identification information of a data authorization table.

[0019]

The 4th data protection system of this invention is characterized by having a means to create a page table, a means to set the page information on the primary storage which each task owns by initial setting of a system as a data protection table per task, and a means to set an attribute as a protection state about the protection page which said data protection table of a page table shows in the system of the operating system use which shares one room between a program.

[0020]

An initialization means for the 5th data protection system of this invention to set up said data protection table in said 4th data protection system, and to set the attribute of said page table as a protection state based on this information, It has the page protection exception-handling means and task change means which will be called if a write-in demand to the page of a protection state is. Said page protection exception-handling means A means to confirm whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, A means to register it if said page is included as a result of a check, the attribute of the applicable page of a page table will be made into an authorized state and said task ID which was being performed will not be registered into a data authorization table, It has the means which makes hibernation the task which was being performed as a result of said check if said page was not included. Said task change means In case a task is changed, the protection page information of the task to which a data protection table corresponds if Task ID is registered into the data authorization table is acquired. The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having a means to eliminate the task ID of said data authorization table.

[0021]

An initialization means for the 6th data protection system of this invention to set up said data protection table in said 4th data protection system, and to set the attribute of said page table as a protection state based on this information, It has the page protection exception-handling means and task change means which will be called if a write-in demand to the page of a protection state is. A page protection exception-handling means A means to confirm whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, A means to make the attribute of the page of a page table concerned into an authorized state if said page is included as a result of a check, and to register the identification information of the page into a data authorization table, It has the means which makes hibernation the task which was being performed if said page was not included as a result of said check. Said task change means If page identification information is registered into the data authorization table in case a task is changed, the attribute of the page to which a page table corresponds will be returned to a protection state, and it will be characterized by having a means to eliminate said page discernment of a data authorization table.

[0022]

The 1st data protection program of this invention is initial setting of a system, and is characterized by have the procedure of set the page information on the primary storage which each task owns as a data protection table per task, and the procedure of create the page table with which the entry corresponding to the address is referred to at the time of primary storage access based on the information on said data protection table, and set the attribute of each page of this as a protection state.

[0023]

The 2nd data protection program of this invention is set to said 1st data protection program. The initialization procedure of setting up said data protection table, creating said page table based on this information, and setting the attribute of each page as a protection state, It has the page protection exception-handling procedure which will be called if a write-in demand to the page of a protection state is, and the task change procedure of performing the change of a task. Said page protection exception-handling procedure The procedure which confirms whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, The procedure of registering it if said page is included as a result of a check, the attribute of the page of a page table concerned will be made into an authorized state and said task ID which was being performed will not be registered into a data authorization table, It has the procedure which makes hibernation the task which was being performed if said page was not included as a result of the

check. In case said task change procedure changes a task, if Task ID is registered into the data authorization table, the protection page information of the correspondence task of a data protection table will be acquired. The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having the procedure which eliminates the task ID of said data authorization table.

[0024]

The 3rd data protection program of this invention is set to said 1st data protection program. The initialization procedure of setting up said data protection table, creating said page table based on this information, and setting the attribute of each page as a protection state, It has the page protection exception-handling procedure which will be called if a write-in demand to the page of a protection state is, and the task change procedure of performing the change of a task. Said page protection exception-handling procedure The procedure which confirms whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included; The procedure of making the attribute of the page of a page table concerned into an authorized state if said page is included as a result of a check, and registering the identification information of the page into a data authorization table, If the identification information of a page is registered into the data authorization table in case it has the procedure which makes hibernation the task which was being performed if said page was not included as a result of the check and said task change procedure changes a task The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having the procedure which eliminates said page discernment of a data authorization table.

[0025]

The 4th data protection program of this invention is characterized by having the procedure which creates a page table, the procedure of setting the page information on the primary storage which is initial setting of a system and each task owns as a data protection table per task, and the procedure of setting an attribute as a protection state about the protection page which said data protection table of a page table shows.

[0026]

The initialization procedure of the 5th data protection program of this invention setting up said data protection table in said 4th data protection program, and setting the attribute of said page table as a protection state based on this information, It has the page protection exception-handling procedure which will be called if a write-in demand to the page of a protection state is, and the task change procedure of performing the change of a task. Said page protection exception-handling procedure The procedure which confirms whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, The procedure of registering it if said page is included as a result of a check, the attribute of the page of a page table concerned will be made into an authorized state and said task ID which was being performed will not be registered into a data authorization table, It has the procedure which makes hibernation the task which was being performed as a result of said check if said page was not included. In case said task change procedure changes a task, the protection page information of the task to which a data protection table corresponds if Task ID is registered into the data authorization table is acquired. The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having the procedure which eliminates the task ID of said data authorization table.

[0027]

The initialization procedure of the 6th data protection program of this invention setting up said data protection table in said 4th data protection program, and setting the attribute of said page table as a protection state based on this information, It has the page protection exception-handling procedure which will be called if a write-in demand to the page of a protection state is, and the task change procedure of performing the change of a task. Said page protection exception-handling procedure The procedure which confirms whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, The procedure of making the attribute of the applicable page of a page table into an authorized state if said page is included as a result of a check, and registering the identification information of the page into a data authorization table, If page identification information is registered into the data authorization table in case it has the procedure which makes hibernation the task which was being performed if said page was not included as a result of said check and said task change procedure changes a task The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having the procedure which eliminates said page discernment of a data authorization table.

[0028]



The initialization procedure in which the 1st data protection approach of this invention carries out initial setting of a system, The page protection exception-handling procedure which will be called if a write-in demand to the page of a protection state is, The procedure of setting the page information on the primary storage in which is equipped with the task change procedure of changing a task, and a task owns said initialization procedure as a data protection table per task, The page table with which the entry corresponding to the address is referred to at the time of primary-storage access is created based on the information on said data protection table. It has the procedure of setting the attribute of each page of this as a protection state. Said page protection exception-handling procedure The procedure which confirms whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, The procedure of registering it if said page is included as a result of a check, the attribute of the page of a page table concerned will be made into an authorized state and said task ID which was being performed will not be registered into a data authorization table, It has the procedure which makes hibernation the task which was being performed if said page was not included as a result of the check. In case said task change procedure changes a task, if Task ID is registered into the data authorization table, the protection page information of the correspondence task of a data protection table will be acquired. The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having the procedure which eliminates the task ID of said data authorization table.

[0029]

The initialization procedure in which the 2nd data protection approach of this invention carries out initial setting of a system, The page protection exception-handling procedure which will be called if a write-in demand to the page of a protection state is, The procedure of setting the page information on the primary storage in which is equipped with the task change procedure of changing a task, and a task owns said initialization procedure as a data protection table per task, The page table with which the entry corresponding to the address is referred to at the time of primary-storage access is created based on the information on said data protection table. It has the procedure of setting the attribute of each page of this as a protection state. Said page protection exception-handling procedure The procedure which confirms whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, The procedure of making the attribute of the page of a page table concerned into an authorized state if said page is included as a result of a check, and registering the identification information of the page into a data authorization table, If the identification information of a page is registered into the data authorization table in case it has the procedure which makes hibernation the task which was being performed if said page was not included as a result of the check and said task change procedure changes a task The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having the procedure which eliminates said page discernment of a data authorization table.

[0030]

The initialization procedure in which the 3rd data protection approach of this invention carries out initial setting of a system, The page protection exception-handling procedure which will be called if a write-in demand to the page of a protection state is, The procedure of setting the page information on the primary storage in which is equipped with the task change procedure of changing a task, and a task owns said initialization procedure as a data protection table per task, According to the information on this data protection table, it has the procedure of setting the attribute of the correspondence page of a page table as a protection state. Said page protection exception-handling procedure The procedure which confirms whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, The procedure of registering it if said page is included as a result of a check, the attribute of the page of a page table concerned will be made into an authorized state and said task ID which was being performed will not be registered into a data authorization table, It has the procedure which makes hibernation the task which was being performed if said page was not included as a result of the check. In case said task change procedure changes a task, if Task ID is registered into the data authorization table, the protection page information of the correspondence task of a data protection table will be acquired. The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having the procedure which eliminates the task ID of said data authorization table.

[0031]

The initialization procedure in which the 4th data protection approach of this invention carries out initial setting of a system, The page protection exception-handling procedure which will be called if a write-in demand to the page of a

protection state is, The procedure of setting the page information on the primary storage in which is equipped with the task change procedure of changing a task, and a task owns said initialization procedure as a data protection table per task, According to the information on this data protection table, it has the procedure of setting the attribute of the correspondence page of a page table as a protection state. Said page protection exception-handling procedure The procedure which confirms whether the page from which ID of the task which was being performed was acquired from said operating system, and the protection page information of the task of a data protection table concerned became said protection exception is included, The procedure of making the attribute of the page of a page table concerned into an authorized state if said page is included as a result of a check, and registering the identification information of the page into a data authorization table, If the identification information of a page is registered into the data authorization table in case it has the procedure which makes hibernation the task which was being performed if said page was not included as a result of the check and said task change procedure changes a task The attribute of the page to which a page table corresponds is returned to a protection state, and it is characterized by having the procedure which eliminates said page discernment of a data authorization table.

[0032]

[Embodiment of the Invention]

Next, the gestalt of operation of this invention is explained to a detail with reference to a drawing. The 1st example of this invention is explained first.

[0033]

Drawing 1 is the block diagram having shown the data protection structure of a system of this invention, and a data protection system is constituted by a real time operating system 1, the data protection table 2, a page table 3, the data authorization table 4, the initialization means 5, and the page protection exception-handling means 6.

[0034]

The initialization means 5 sets the task (it rewrites) ID which owns the page address of the data which were decided beforehand, and to protect, pagination (die length), and its data as the data protection table 2 per task ID.

[0035]

Next, the initialization means 5 creates a page table 3 according to the specification of MMU (memory management unit) based on the information on the data protection table 2.

[0036]

By the primary-storage access request which programs also including a real time operating system 1 perform, the entry of the page table 3 corresponding to the access address is referred to.

[0037]

A real time operating system 1 has the task management means 11 and the task change means 12, and the task change means 12 has the page information change means 121.

[0038]

The task management means 11 determines the task performed next according to the task information and the priority under activation.

[0039]

When a task change occurs, the task change means 12 is referred to data authorization table 4 in order to judge whether the data from which the task which was being performed with the page information change means 121 is protected were accessed.

[0040]

If ID of a task is registered into the data authorization table 4, the protection page which the task owns will consider that it was made the authorized state by the page information change means 121 at the task activation period.

[0041]

And with reference to the page information which the task which was performing the data protection table 2 protects, according to it, the attribute of the applicable entry of a page table 3 is made into a protection state (it is return to a protection state), the information on the data authorization table 4 is eliminated, and the task change means 12 acquires the task performed next from the task management means 11, and changes it to the task.

[0042]

When Task ID is not registered into the data authorization table 4, it considers that the task which was being performed has not accessed a protection page, the task performed next from the task management means 11 is acquired, and it changes to the task.

[0043]



When a page protection exception occurs, by the primary-storage access request which a program performs, the entry of the page table 3 corresponding to the access address is referred to, if the attribute is [ a demand ] writing in a protection state, it will become a page protection exception and the page protection exception-handling means 6 will be called.

[0044]

It judges whether the page protection exception-handling means 6 contains the page which the page protection exception generated [ the protection page information which acquired the task ID which was being performed before exception handling, made it the key, accessed the data protection table 2, and was acquired from the task management means 11 ].

[0045]

The information (the task ID under activation) which shows that the attribute of the page address which the page protection exception of a page table 3 generated was made into the authorized state when in agreement, and the task under activation on the data authorization table 4 made its protection page the authorized state is written, and activation of a task is continued. Under the present circumstances, a postscript will not be added if the task ID under activation on the data authorization table 4 is already registered. When not in agreement, error information is written, and a task is made into hibernation.

[0046]

The above-mentioned initialization means 5, the page protection exception-handling means 6, and each means of a real time operating system 1 are realized by the program procedure in the terminal (a personal digital assistant and a cellular phone with an information processing function are also included) and information processor which realize a system.

[0047]

In addition, when accessing a primary storage only by the real address mode by the system using a real time operating system 1, it is not necessary to establish the logical address information on each entry of a page table 3.

[0048]

Next, actuation of this example is explained with reference to a drawing. Drawing 2 is a flow chart which shows actuation of a data protection system, and the procedure of a data protection program and the data protection approach.

[0049]

The protected data which perform an initialization process first, and set the first task to task #1 with reference to drawing 2, and this owns are accessed, and the case where task #1 was performed, changed to task #2, and other protection pages of task #1 grade carry out a write request faultily is explained.

[0050]

The initialization means 5 registers the page address and pagination of a page to protect into the data protection table 2 per task (step 1). Based on the information on the data protection table 2, it doubles with the specification of MMU, a page table 3 is created, and the attribute of each entry is set as protection (step 2).

[0051]

The task which the task management means 11 performs next according to a priority is decided (step 3). (change generating to task #1) Since it confirms whether the task change means 12 has registration information in the data authorization table 4 and is not registered per beginning (step 4), it changes to the following task (task #1) immediately, and this is performed.

[0052]

A page protection exception occurs in primary-storage access (writing) of task #1 (step 7).

[0053]

The task ID (#1) which the page protection exception-handling means 6 was performing is acquired from the task management means 11, and the protection page information of ID#1 of the data protection table 2 is acquired (step 8).

[0054]

Whether protection page information contains the page which the exception generated judges, it makes an authorized state the attribute which is the page which the exception generated since it is contained (step 9), and since the task ID under activation on the data authorization table 4 (#1) is not registered, this is registered (step 10).

[0055]

Since it judges whether it is the terminating condition of a system as activation of task #1 being completed and there is no terminating condition (step 13), the change to the following task (#2) occurs (step 3). (step 11)

[0056]

Since it confirms whether the task change means 12 has registration information in the data authorization table 4 and ID#1 is registered, this is made into a key, the protection page information (page address) of task ID#1 is acquired from the data protection table 2, the attribute information on the page address 001 (entry #1) of a page table 3 is returned to a

protection state, and the information on the data authorization table 4 is eliminated (step 5).

[0057]

It changes to the following task (#2), this is performed (step 6), task #2 require the writing to the protection page of task #1 faultily, and a page protection exception generates the task change means 12 (step 7).

[0058]

The page protection exception-handling means 6 acquires the task ID (#2) which was being performed, and acquires the protection page information of ID#2 of the data protection table 2 (step 8).

[0059]

And it judges with the page which the exception generated not being contained in this, and supposes that the write-in demand to the protection page of other (step 9) tasks was performed, and error information is written and a task is made into hibernation during activation (step 12).

[0060]

In addition, error information may be serial, and may be taken out outside, may be saved in memory, or may be displayed on a display. Except MMU is sufficient as memory protection hardware.

[0061]

Next, the 2nd example of this invention is explained. In this example, in case a program etc. is loaded to a primary storage, the main storage area for a program or data is assigned by MMU or the initialization means 5, and a page table 3 is created according to this information.

[0062]

The initialization means 5 sets the task (it rewrites) ID which owns the page address of the data to protect, pagination (die length), and its data as the data protection table 2 per task ID.

[0063]

Next, the initialization means 5 sets the attribute information which is the page which the protection page information of the data protection table 2 specifies among the entries of a page table 3 as a protection state. Other functions and processings are the same as that of said 1st example.

[0064]

Next, the 3rd example of this invention is explained. In this example, when the attribute of the page from which the page protection exception-handling means 6 became the exception of a page table 3 is set as an authorized state, not the task ID under activation but page discernment (a page address or page table entry number) is registered into the data authorization table 4 (refer to drawing 3 ).

[0065]

When one task carries out sequential access to its protection page and an authorized-state setup by the page protection exception-handling means 6 is performed each time, the sequential postscript of the page discernment is carried out at the data authorization table 4. [ two or more ]

[0066]

Moreover, in case the task change means 12 changes a task, the registration information existence of the data authorization table 4 is checked, if it is, the attribute which is the page which it shows will be set as a protection state, and the page identification information of the data authorization table 4 will be eliminated.

[0067]

If two or more page identification information is registered into the data authorization table 4, the above-mentioned actuation will be repeated and will be performed.

[0068]

Other functions thru/or procedure of a means is the same as that of the 1st example or the 2nd example.

[0069]

[Effect of the Invention]

According to this invention, except when a page protection exception occurs, rewriting of page information does not occur. For this reason, page table rewriting time amount and the processing time by the mistake hit of a page table cache are made few.

[0070]

Since the page which did not change an attribute into authorization unconditionally about the protection page of a large number which the following task owns especially by task change, but actually rewrote, and the demand generated is processed, the real-time operation of two or more tasks is carried out by time sharing, also in the small personal digital assistant and small cellular phone of a task with which throughput is restricted per time, excessive processing concerning

data protection is not performed, but the processing time can be lessened, and the simultaneous-processing nature of two or more tasks can also be maintained.

[0071]

Moreover, since the initialization means of a system sets the protection page which each program area and it own as a data protection table, and develops the protection page information to a page table, each page attribute is made into a protection state and only its page is permitted temporarily, the protection feature of data can be added, without correcting the program which is carrying out present condition use. [ of write-in access ] [ inner ]

[Brief Description of the Drawings]

[Drawing 1] The block diagram having shown the data protection structure of a system of this invention.

[Drawing 2] The flow chart which shows actuation of the data protection system of this invention, and the procedure of a data protection program and the data protection approach.

[Drawing 3] The block diagram showing the contents of the data authorization table 4 of the 3rd example of this invention.

[Description of Notations]

1 Real Time Operating System

11 Task Management Means

12 Task Change Means

121 Page Information Change Means

2 Data Protection Table

3 Page Table

4 Data Authorization Table

5 Initialization Means

6 Page Protection Exception-Handling Means

---

[Translation done.]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-157751

(P2004-157751A)

(43) 公開日 平成16年6月3日(2004.6.3)

(51) Int. Cl.<sup>7</sup>

G06F 12/14

G06F 9/46

F 1

G06F 12/14 310A

G06F 9/46 340B

G06F 9/46 340F

テーマコード (参考)

5B017

5B098

審査請求 未請求 請求項の数 16 OL (全 15 頁)

(21) 出願番号 特願2002-322604 (P2002-322604)  
 (22) 出願日 平成14年11月6日 (2002.11.6)

(71) 出願人 000004237  
 日本電気株式会社  
 東京都港区芝五丁目7番1号  
 (74) 代理人 100109313  
 弁理士 机 昌彦  
 (74) 代理人 100085268  
 弁理士 河合 信明  
 (74) 代理人 100111637  
 弁理士 谷澤 靖久  
 (72) 発明者 深川 好美  
 東京都港区芝五丁目7番1号  
 日本電気株式会社内  
 Fターム(参考) 5B017 AA02 BA04 CA01  
 5B098 AA03 GA02 GA04 GB05 GB11  
 GD03 GD14 JJ03

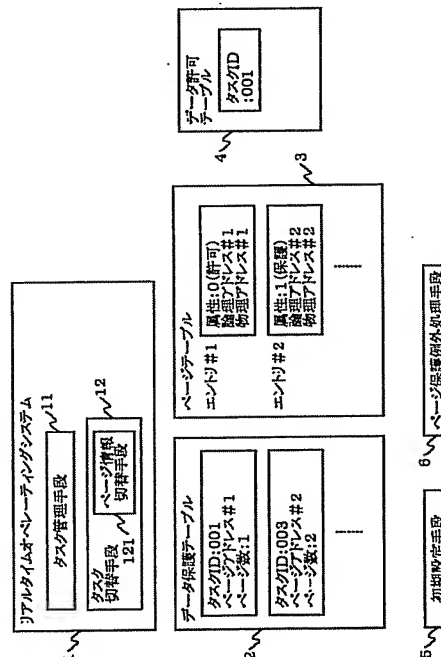
(54) 【発明の名称】 データ保護システム、データ保護プログラム及びデータ保護方法

(57) 【要約】

【課題】 リアルタイムOS利用システムで、タスクが所有するデータ等を、テーブルを含むアクセス機構により保護する従来のシステムでは、処理時間が長くなる場合がある、金物増加量が多くなるといった問題があった。

【解決手段】 初期設定手段5が、個々タスクが所有するページ情報をタスク単位でデータ保護テーブル2に設定しこの情報を元にページテーブル3を作成し各ページ属性を保護に設定し、ページ保護例外処理手段6が呼び出されるとデータ保護テーブル2の実行中タスク対応の保護ページ情報が例外となったページを含むかチェックし、含めば該ページ属性を許可にしデータ許可テーブル4にタスクIDを登録し、含まなければ実行中タスクを休止状態にし、タスク切替手段12が、タスク切替え時、前記登録されたタスクIDでデータ保護テーブル2より保護ページ情報を取得し、対応するページの属性を保護状態に戻す。

【選択図】 図1



## 【特許請求の範囲】

## 【請求項 1】

一つのメモリ空間をプログラムで共有するオペレーティングシステム利用のシステムにおいて、システムの初期設定で、個々のタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手段と、主記憶アクセス時そのアドレスに対応するエントリが参照されるページテーブルを前記データ保護テーブルの情報を元に作成し、これの各ページの属性を保護状態に設定する手段を有することを特徴とするデータ保護システム。

## 【請求項 2】

前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルを作成し、各ページの属性を保護状態に設定する初期設定手段と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手段と、タスク切替手段を備え、前記ページ保護例外処理手段は、実行していたタスクの ID を前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手段と、チェックの結果前記ページを含めばページテーブルの該当ページの属性を許可状態にし、前記実行していたタスク ID がデータ許可テーブル 4 に登録されてなければそれを登録する手段と、前記チェックの結果、前記ページを含まなければ実行していたタスクを休止状態にする手段を有し、前記タスク切替手段は、タスクを切り替える際に、データ許可テーブルにタスク ID が登録されていればデータ保護テーブルの対応するタスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスク ID を消去する手段を有することを特徴とする請求項 1 記載のデータ保護システム。

## 【請求項 3】

前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルを作成し、各ページの属性を保護状態に設定する初期設定手段と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手段と、タスク切替手段を備え、前記ページ保護例外処理手段は、実行していたタスクの ID を前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手段と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手段と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手段を有し、前記タスク切替手段は、タスクを切り替える際に、データ許可テーブルにページ識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別情報を消去する手段を有することを特徴とする請求項 1 記載のデータ保護システム。

## 【請求項 4】

一つのメモリ空間をプログラムで共有するオペレーティングシステム利用のシステムにおいて、ページテーブルを作成する手段と、システムの初期設定で、個々のタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手段と、ページテーブルの、前記データ保護テーブルが示す保護ページについて属性を保護状態に設定する手段を有することを特徴とするデータ保護システム。

## 【請求項 5】

前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルの属性を保護状態に設定する初期設定手段と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手段とタスク切替手段を備え、前記ページ保護例外処理手段は、実行していたタスクの ID を前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手段と、チェックの結果前記ページを含めばページテーブルの該当ページの属性を許可状態にし、前記実行していたタスク ID がデータ許可テーブルに登録されてなければそれを登録する手段と、前記チェックの結果、前記ページを含まなければ実行していたタスクを休止

状態にする手段を有し、前記タスク切替手段は、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応するタスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手段を有することを特徴とする請求項4記載のデータ保護システム。

【請求項6】

前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルの属性を保護状態に設定する初期設定手段と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手段とタスク切替手段を備え、ページ保護例外処理手段は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手段と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手段と、前記チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手段を有し、前記タスク切替手段は、タスクを切り替える際に、データ許可テーブルにページ識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手段を有することを特徴とする請求項4記載のデータ保護システム。

10

【請求項7】

システムの初期設定で、個々のタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、主記憶アクセス時そのアドレスに対応するエントリが参照されるページテーブルを前記データ保護テーブルの情報を元に作成し、これの各ページの属性を保護状態に設定する手順を有することを特徴とするデータ保護プログラム。

20

【請求項8】

前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルを作成し、各ページの属性を保護状態に設定する初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応タスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手順を有することを特徴とする請求項7記載のデータ保護プログラム。

30

【請求項9】

前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルを作成し、各ページの属性を保護状態に設定する初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順とタスクの切替を行うタスク切替手順を備え、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにページの識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手順を有することを特徴とする請求項7記載のデータ保護プログラム。

40

50



## 【請求項 1 0】

ページテーブルを作成する手順と、システムの初期設定で、個々のタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、ページテーブルの、前記データ保護テーブルが示す保護ページについて属性を保護状態に設定する手順を有することを特徴とするデータ保護プログラム。

## 【請求項 1 1】

前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルの属性を保護状態に設定する初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手順と、前記チェックの結果、前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応するタスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手順を有することを特徴とする請求項 1 0 記載のデータ保護プログラム。

## 【請求項 1 2】

前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルの属性を保護状態に設定する初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手順と、前記チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにページ識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手順を有することを特徴とする請求項 1 0 記載のデータ保護プログラム。

## 【請求項 1 3】

システムの初期設定をする初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記初期設定手順はタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、主記憶アクセス時そのアドレスに対応するエントリが参照されるページテーブルを前記データ保護テーブルの情報を元に作成し、これの各ページの属性を保護状態に設定する手順を有し、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応タスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手順を有することを特徴とするデータ保護方法。

## 【請求項 1 4】

システムの初期設定をする初期設定手順と、保護状態のページへの書込要求があれば呼び

出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記初期設定手順はタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、主記憶アクセス時そのアドレスに対応するエントリが参照されるページテーブルを前記データ保護テーブルの情報を元に作成し、これの各ページの属性を保護状態に設定する手順を有し、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにページの識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手順を有することを特徴とするデータ保護方法。

10

**【請求項15】**

システムの初期設定をする初期設定手順と、保護状態のページへの書込要求が有れば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記初期設定手順はタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、このデータ保護テーブルの情報に従って、ページテーブルの対応ページの属性を保護状態に設定する手順を有し、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応タスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手順を有することを特徴とするデータ保護方法。

20

**【請求項16】**

システムの初期設定をする初期設定手順と、保護状態のページへの書込要求が有れば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記初期設定手順はタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、このデータ保護テーブルの情報に従って、ページテーブルの対応ページの属性を保護状態に設定する手順を有し、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにページの識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手順を有することを特徴とするデータ保護方法。

30

40

**【発明の詳細な説明】****【0001】****【発明の属する技術分野】**

本発明は、リアルタイムオペレーティングシステムの様に、主記憶上に全プログラムとデータをロードしておきメモリ空間を全てのプログラムで共有しているオペレーティングシステムを利用する際にプログラムのデータを保護するシステム、プログラムのデータを保護するプログラム、保護方法に関し、特にこの様なオペレーティングシステムを利用する際に、プログラムの不具合等で他のプログラムやタスクのデータが書き換えられることを

50

防止するデータ保護システム、データ保護プログラム及びデータ保護方法に関する。

【0002】

【従来の技術】

従来、仮想記憶を備えたオペレーティングシステムではプロセス毎にアドレス空間を持ち、プロセスの切替毎にページテーブルを更新する。これにより、カレントプロセスから別のプロセスのデータを書き換えることは起きない。

【0003】

しかし、リアルタイムシステムで利用するリアルタイムオペレーティングシステムは高速な処理が必要なため、主記憶メモリ上に全プログラムとデータをロードしておきメモリ空間を全てのプログラムで共有している。

【0004】

また、プログラムとデータのアドレスは物理アドレスと一致している。

【0005】

よって、プログラムの不具合による不適当なアドレスへのアクセスを検出できない。

【0006】

一方これに類似した問題を改善する技術としてメモリ保護装置がある（例えば、特許文献1参照）。

【0007】

このメモリ保護装置は、各メモリブロックに対応して保護情報を格納する複数のメモリ保護情報記憶手段と、あるメモリブロックに関する属性情報を記憶するカレントキー情報記憶手段とを備え、あるメモリブロックをアクセスする前に予め、該メモリブロックに対応するメモリ保護情報記憶手段に保護キーを設定し、該メモリブロックに関する属性キーをカレントキー情報記憶手段に設定しておき、メモリブロックへのアクセスがある度に該メモリアccessと並行して、メモリ保護記憶手段内の該メモリアドレスに対応するメモリブロックの保護キーとカレントキー情報記憶手段内の属性キーとを比較し、予め定められた条件を満足すれば該メモリアccessを許容し、満足しなければ該メモリアccessを禁止してアクセス違反が生じたことを外部に通知するメモリ保護装置である。

【0008】

ここで保護キーレジスタのメモリブロック上位アドレスが一致し、かつカレントキーレジスタと保護キーレジスタのプロセスIDが一致すればアクセスを許可する。

【0009】

又、メモリ保護テーブルをメモリブロックを格納する一般のメモリから分離して、メモリ保護テーブルとメモリブロックとが同時アクセス出来るようにすることによって処理能力を低下させることなくメモリ保護チェックを行うものである。

【0010】

【特許文献1】

特開平5-134930号公報（段落【0008】、【0014】、【0054】～【0056】）

【0011】

【発明が解決しようとする課題】

従って、上記メモリ保護装置では、メモリ保護テーブルの各エントリがプロセスIDを保持しており、1ビットの保護ビットを設ける場合よりメモリサイズが大きくなり、又一般メモリとは分離した別のメモリ等であり、その分金物量が増えると言う問題がある。

【0012】

少なくとも、携帯端末等の小型装置におけるデータの保護システムには向かない。

【0013】

また、メモリ保護テーブルへのプロセスID等の設定は、あるメモリブロックをアクセスする前に予め設定するが、初期設定で全エントリの設定を纏めて行う手段はなく、初期に全てのプログラムを主記憶にロードし、データ域を確保して以降そのメモリマップで動作するシステムには向かない。

10

20

30

40

50

## 【0014】

本発明の目的は、リアルタイムオペレーティングシステムの様に、主記憶メモリ上に全プログラムとデータをロードしておきメモリ空間を全てのプログラムで共有しているオペレーティングシステムを利用したシステムで、個々のプログラムの所有する（書き換えできる）領域を保護するシステム、保護するためのプログラム及び方法を提供するものである。

## 【0015】

特に、主記憶アクセスに関する処理時間増加を少なくでき、オペレーティングシステム配下のプログラムを変更することなく、又、小型の端末や情報処理装置にも適用できるデータ保護システム、保護プログラム及び方法を提供するものである。

10

## 【0016】

## 【課題を解決するための手段】

本発明の第1のデータ保護システムは、一つのメモリ空間をプログラムで共有するオペレーティングシステム利用のシステムにおいて、システムの初期設定で、個々のタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手段と、主記憶アクセス時そのアドレスに対応するエントリが参照されるページテーブルを前記データ保護テーブルの情報を元に作成し、これの各ページの属性を保護状態に設定する手段を有することを特徴とする。

## 【0017】

本発明の第2のデータ保護システムは、前記第1のデータ保護システムに於いて、前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルを作成し、各ページの属性を保護状態に設定する初期設定手段と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手段と、タスク切替手段を備え、前記ページ保護例外処理手段は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手段と、チェックの結果前記ページを含めばページテーブルの該当ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブル4に登録されてなければそれを登録する手段と、前記チェックの結果、前記ページを含まなければ実行していたタスクを休止状態にする手段を有し、前記タスク切替手段は、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応するタスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手段を有することを特徴とする。

20

30

## 【0018】

本発明の第3のデータ保護システムは、前記第1のデータ保護システムに於いて、前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルを作成し、各ページの属性を保護状態に設定する初期設定手段と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手段と、タスク切替手段を備え、前記ページ保護例外処理手段は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手段と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手段と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手段を有し、前記タスク切替手段は、タスクを切り替える際に、データ許可テーブルにページ識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別情報を消去する手段を有することを特徴とする。

40

## 【0019】

本発明の第4のデータ保護システムは、一つのメモリ空間をプログラムで共有するオペレーティングシステム利用のシステムにおいて、ページテーブルを作成する手段と、システムの初期設定で、個々のタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手段と、ページテーブルの、前記データ保護テーブルが示す保護ペ

50

ージについて属性を保護状態に設定する手段を有することを特徴とする。

【0020】

本発明の第5のデータ保護システムは、前記第4のデータ保護システムに於いて、前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルの属性を保護状態に設定する初期設定手段と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手段とタスク切替手段を備え、前記ページ保護例外処理手段は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手段と、チェックの結果前記ページを含めばページテーブルの該当ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手段と、前記チェックの結果、前記ページを含まなければ実行していたタスクを休止状態にする手段を有し、前記タスク切替手段は、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応するタスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手段を有することを特徴とする。

10

【0021】

本発明の第6のデータ保護システムは、前記第4のデータ保護システムに於いて、前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルの属性を保護状態に設定する初期設定手段と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手段とタスク切替手段を備え、ページ保護例外処理手段は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手段と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手段と、前記チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手段を有し、前記タスク切替手段は、タスクを切り替える際に、データ許可テーブルにページ識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手段を有することを特徴とする。

20

【0022】

本発明の第1のデータ保護プログラムは、システムの初期設定で、個々のタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、主記憶アクセス時そのアドレスに対応するエントリが参照されるページテーブルを前記データ保護テーブルの情報を元に作成し、これの各ページの属性を保護状態に設定する手順を有することを特徴とする。

30

【0023】

本発明の第2のデータ保護プログラムは、前記第1のデータ保護プログラムに於いて、前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルを作成し、各ページの属性を保護状態に設定する初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応タスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手順を有することを特徴とする。

40

【0024】

50

本発明の第3のデータ保護プログラムは、前記第1のデータ保護プログラムに於いて、前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルを作成し、各ページの属性を保護状態に設定する初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順とタスクの切替を行うタスク切替手順を備え、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにページの識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手順を有することを特徴とする。

10

## 【0025】

本発明の第4のデータ保護プログラムは、ページテーブルを作成する手順と、システムの初期設定で、個々のタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、ページテーブルの、前記データ保護テーブルが示す保護ページについて属性を保護状態に設定する手順を有することを特徴とする。

## 【0026】

本発明の第5のデータ保護プログラムは、前記第4のデータ保護プログラムに於いて、前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルの属性を保護状態に設定する初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手順と、前記チェックの結果、前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応するタスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手順を有することを特徴とする。

20

30

## 【0027】

本発明の第6のデータ保護プログラムは、前記第4のデータ保護プログラムに於いて、前記データ保護テーブルの設定を行い、この情報を元に前記ページテーブルの属性を保護状態に設定する初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの該当ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手順と、前記チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにページ識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手順を有することを特徴とする。

40

## 【0028】

本発明の第1のデータ保護方法は、システムの初期設定をする初期設定手順と、保護状態のページへの書込要求があれば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記初期設定手順はタスクが所有する主記憶上のページ情報

50



をタスク単位でデータ保護テーブルに設定する手順と、主記憶アクセス時そのアドレスに対応するエントリが参照されるページテーブルを前記データ保護テーブルの情報を元に作成し、これの各ページの属性を保護状態に設定する手順を有し、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応タスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手順を有することを特徴とする。 10

#### 【0029】

本発明の第2のデータ保護方法は、システムの初期設定をする初期設定手順と、保護状態のページへの書込要求が有れば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記初期設定手順はタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、主記憶アクセス時そのアドレスに対応するエントリが参照されるページテーブルを前記データ保護テーブルの情報を元に作成し、これの各ページの属性を保護状態に設定する手順を有し、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにページの識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手順を有することを特徴とする。 20

#### 【0030】

本発明の第3のデータ保護方法は、システムの初期設定をする初期設定手順と、保護状態のページへの書込要求が有れば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記初期設定手順はタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、このデータ保護テーブルの情報に従って、ページテーブルの対応ページの属性を保護状態に設定する手順を有し、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、前記実行していたタスクIDがデータ許可テーブルに登録されてなければそれを登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにタスクIDが登録されていればデータ保護テーブルの対応タスクの保護ページ情報を取得し、ページテーブルの対応するページの属性を保護状態に戻し、前記データ許可テーブルのタスクIDを消去する手順を有することを特徴とする。 30 40

#### 【0031】

本発明の第4のデータ保護方法は、システムの初期設定をする初期設定手順と、保護状態のページへの書込要求が有れば呼び出されるページ保護例外処理手順と、タスクの切替を行うタスク切替手順を備え、前記初期設定手順はタスクが所有する主記憶上のページ情報をタスク単位でデータ保護テーブルに設定する手順と、このデータ保護テーブルの情報に従って、ページテーブルの対応ページの属性を保護状態に設定する手順を有し、前記ページ保護例外処理手順は、実行していたタスクのIDを前記オペレーティングシステムより 50

取得し、データ保護テーブルの当該タスクの保護ページ情報が前記保護例外となったページを含むかをチェックする手順と、チェックの結果前記ページを含めばページテーブルの当該ページの属性を許可状態にし、そのページの識別情報をデータ許可テーブルに登録する手順と、チェックの結果前記ページを含まなければ実行していたタスクを休止状態にする手順を有し、前記タスク切替手順が、タスクを切り替える際に、データ許可テーブルにページの識別情報が登録されていれば、ページテーブルの対応するページの属性を保護状態に戻し、データ許可テーブルの前記ページ識別を消去する手順を有することを特徴とする。

【0032】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して詳細に説明する。先ず本発明の第1実施例を説明する。

【0033】

図1は本発明のデータ保護システムの構成を示したブロック図であり、データ保護システムは、リアルタイムオペレーティングシステム1、データ保護テーブル2、ページテーブル3、データ許可テーブル4、初期設定手段5、ページ保護例外処理手段6により構成される。

【0034】

初期設定手段5は予め決めた保護するデータのページアドレスとページ数（長さ）とそのデータを所有する（書き換える）タスクIDとをタスクID単位でデータ保護テーブル2に設定する。

【0035】

次に初期設定手段5はデータ保護テーブル2の情報をもとにMMU（メモリマネージメントユニット）の仕様に合わせてページテーブル3を作成する。

【0036】

リアルタイムオペレーティングシステム1も含めてプログラムが行う主記憶アクセス要求で、アクセスアドレスに対応したページテーブル3のエントリが参照される。

【0037】

リアルタイムオペレーティングシステム1はタスク管理手段11とタスク切替手段12を持ち、タスク切替手段12はページ情報切替手段121を有する。

【0038】

タスク管理手段11は実行中のタスク情報とプライオリティに合わせて次に実行するタスクを決める。

【0039】

タスク切替手段12はタスク切替が発生した場合、ページ情報切替手段121により実行していたタスクが保護されているデータにアクセスしていたか判断するためデータ許可テーブル4参照する。

【0040】

ページ情報切替手段121はデータ許可テーブル4にタスクのIDが登録されていれば、そのタスクが所有する保護ページがそのタスク実行期間に許可状態にされたと見なす。

【0041】

そしてデータ保護テーブル2の実行していたタスクの保護するページ情報を参照し、それに従ってページテーブル3の該当エントリの属性を保護状態にし（保護状態に戻し）、データ許可テーブル4の情報を消去し、タスク切替手段12はタスク管理手段11より次に実行するタスクを取得し、そのタスクに切替える。

【0042】

データ許可テーブル4にタスクIDが登録されていない場合は、実行していたタスクが保護ページにアクセスしていないと見なし、タスク管理手段11より次に実行するタスクを取得し、そのタスクに切替える。

【0043】

10

20

30

40

50

ページ保護例外が発生した場合、即ち、プログラムが行う主記憶アクセス要求で、アクセスアドレスに対応したページテーブル3のエントリが参照されその属性が保護状態で、要求が書き込みであればページ保護例外となりページ保護例外処理手段6が呼び出される。

【0044】

ページ保護例外処理手段6はタスク管理手段11より例外処理前に実行していたタスクIDを取得し、それをキーとしデータ保護テーブル2にアクセスし取得した保護ページ情報が、ページ保護例外が発生したページを含むか判断する。

【0045】

一致している場合ページテーブル3のページ保護例外が発生したページアドレスの属性を許可状態とし、データ許可テーブル4に実行中のタスクが自分の保護ページを許可状態にしたことを示す情報（実行中のタスクID）を書きタスクの実行を継続する。この際データ許可テーブル4に実行中のタスクIDが既に登録されていれば追記しない。一致しない場合はエラー情報を書き、タスクを休止状態にする。

10

【0046】

上記初期設定手段5、ページ保護例外処理手段6、リアルタイムオペレーティングシステム1の各手段は、システムを実現する端末（携帯端末、情報処理機能を持つ携帯電話も含む）や情報処理装置におけるプログラム手順により実現される。

【0047】

尚、リアルタイムオペレーティングシステム1を利用するシステムで、主記憶には実アドレスモードでしかアクセスしない場合は、ページテーブル3の各エントリの論理アドレス情報は設ける必要はない。

20

【0048】

次に、本実施例の動作について図面を参照して説明する。図2はデータ保護システムの動作やデータ保護プログラム、データ保護方法の手順を示すフローチャートである。

【0049】

図2を参照し、先ず初期設定処理を行い最初のタスクをタスク#1としこれが所有する保護されたデータにアクセスし、タスク#1が実行されタスク#2に切り替わり不具合でタスク#1等の他の保護ページの書き込み要求した場合について説明する。

【0050】

初期設定手段5は保護するページのページアドレスとページ数をタスク単位でデータ保護テーブル2に登録する（ステップ1）。データ保護テーブル2の情報を元に、MMUの仕様に合わせページテーブル3を作成し各エントリの属性を保護に設定する（ステップ2）。

30

【0051】

タスク管理手段11がプライオリティに従って次に実行するタスクを決める（タスク#1への切替発生）（ステップ3）。タスク切替手段12はデータ許可テーブル4に登録情報が有るかチェックし、最初につき登録されてないので（ステップ4）、直ぐに次のタスク（タスク#1）に切替えこれが実行される。

【0052】

タスク#1の主記憶アクセス（書き込み）でページ保護例外が発生する（ステップ7）。

40

【0053】

ページ保護例外処理手段6が実行していたタスクID（#1）をタスク管理手段11より取得し、データ保護テーブル2のID#1の保護ページ情報を取得する（ステップ8）。

【0054】

保護ページ情報が、例外が発生したページを含むか判定し、含まれるので（ステップ9）、例外が発生したページの属性を許可状態にし、データ許可テーブル4に実行中のタスクID（#1）が登録されてないのでこれを登録する（ステップ10）。

【0055】

タスク#1の実行が終了すると（ステップ11）、システムの終了条件かを判定し、終了条件はないので（ステップ13）、次のタスク（#2）への切替が発生する（ステップ3

50

）。

【0056】

タスク切替手段12はデータ許可テーブル4に登録情報が有るかチェックし、ID#1が登録されているので、これをキーとしデータ保護テーブル2よりタスクID#1の保護ページ情報（ページアドレス）を取得し、ページテーブル3のページアドレス001（エントリ#1）の属性情報を保護状態に戻し、データ許可テーブル4の情報を消去する（ステップ5）。

【0057】

タスク切替手段12は次のタスク（#2）に切替えこれが実行され（ステップ6）、タスク#2が不具合でタスク#1の保護ページへの書き込みを要求しページ保護例外が発生する（ステップ7）。 10

【0058】

ページ保護例外処理手段6は実行していたタスクID（#2）を取得し、データ保護テーブル2のID#2の保護ページ情報を取得する（ステップ8）。

【0059】

そして、これには、例外が発生したページが含まれないと判定し（ステップ9）他タスクの保護ページへの書込要求が行われたとし、エラー情報を書き実行中タスクを休止状態にする（ステップ12）。

【0060】

尚、エラー情報はシリアルで外部に出してもメモリに保存してもディスプレイに表示してもよい。メモリ保護ハードウェアはMMU以外でもよい。 20

【0061】

次に本発明の第2実施例を説明する。本実施例ではプログラム等が主記憶にロードされる際にプログラムやデータ用の主記憶領域がMMU或いは初期設定手段5により割り付けられ、この情報に従ってページテーブル3が作成される。

【0062】

初期設定手段5は保護するデータのページアドレスとページ数（長さ）とそのデータを所有する（書き換える）タスクIDとをタスクID単位でデータ保護テーブル2に設定する。

【0063】

次に初期設定手段5はページテーブル3のエントリの内、データ保護テーブル2の保護ページ情報が指定するページの属性情報を保護状態に設定する。他の機能や処理は前記第1の実施例と同様である。 30

【0064】

次に本発明の第3実施例を説明する。本実施例ではページ保護例外処理手段6が、ページテーブル3の例外となったページの属性を許可状態に設定した際に、データ許可テーブル4には、実行中のタスクIDでなく、ページ識別（ページアドレス或いはページテーブルエントリ番号）を登録する（図3参照）。

【0065】

一つのタスクが複数の自分の保護ページに順次アクセスし、其の都度ページ保護例外処理手段6による許可状態設定が行われる場合は、データ許可テーブル4には、ページ識別が順次追記される。 40

【0066】

又、タスク切替手段12がタスクを切り替える際にデータ許可テーブル4の登録情報有無をチェックし、あればそれが示すページの属性を保護状態に設定し、データ許可テーブル4のページ識別情報を消去する。

【0067】

データ許可テーブル4に複数のページ識別情報が登録されていれば、上記動作を繰り返す行う。

【0068】

他の手段の機能ないし処理手順は第1の実施例、或いは第2の実施例と同様である。

【0069】

【発明の効果】

本発明によれば、ページ保護例外が発生したとき以外はページ情報の書換が発生しない。このためページテーブル書換時間、ページテーブルキャッシュのミスヒットによる処理時間が少なく出来る。

【0070】

特にタスク切替で次のタスクが所有する多数の保護ページについて無条件で属性を許可に変更するのではなく実際に書き換え要求が発生したページを処理するので、複数のタスクを時分割でリアルタイム処理しタスクの1回当たり処理量が限られる小型の携帯端末や携帯電話においても、データ保護に係わる余分な処理を行わず処理時間を少なくでき、複数タスクの同時処理性も維持出来る。

【0071】

また、システムの初期設定手段が個々のプログラムエリアやその所有する保護ページをデータ保護テーブルに設定し、その保護ページ情報をページテーブルに展開し、各ページ属性を保護状態とし、書込アクセスの内自分のページのみ一時許可するので、現状使用しているプログラムを修正することなくデータの保護機能を追加することが出来る。

【図面の簡単な説明】

【図1】本発明のデータ保護システムの構成を示したブロック図。

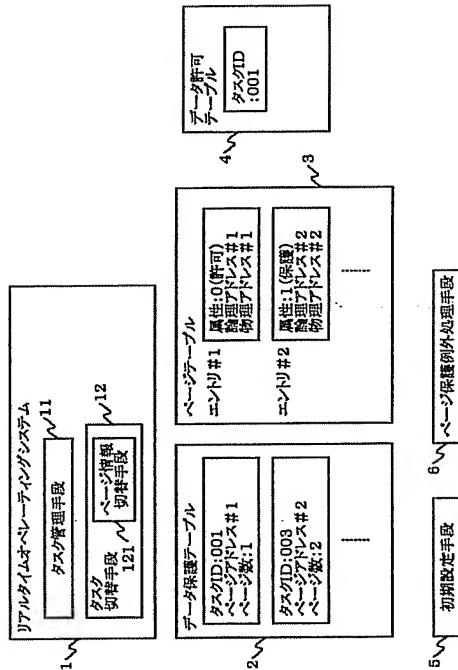
【図2】本発明のデータ保護システムの動作やデータ保護プログラム、データ保護方法の手順を示すフローチャート。

【図3】本発明の第3の実施例のデータ許可テーブル4の内容を示すブロック図。

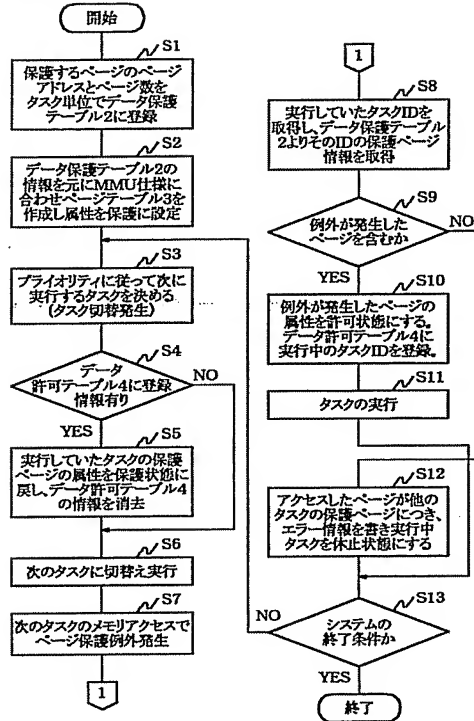
【符号の説明】

- 1 リアルタイムオペレーティングシステム
- 1 1 タスク管理手段
- 1 2 タスク切替手段
- 1 2 1 ページ情報切替手段
- 2 データ保護テーブル
- 3 ページテーブル
- 4 データ許可テーブル
- 5 初期設定手段
- 6 ページ保護例外処理手段

【図 1】



【図 2】



【図 3】

